

CLAIMS:

1. Reproducing apparatus (1) for reproducing content stored in encrypted form on a record carrier (2), said record carrier (2) further storing a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and an encrypted region key (RK) for decrypting said content, comprising:

- 5 - a region code storage means (10) for storing a device region code (RCD),
- a device key storage means (11) for storing a device key (DK), said device key (DK) being different for all regions,
- a carrier region code reading means (12) for reading said carrier region code (RCC) from said record carrier (2),
- 10 - a region code check unit (13) for checking if said carrier region code (RCC) matches said device region code (RCD),
- a region key reading means (14) for reading said encrypted region key (RK) from said record carrier (2),
- a region key decryption means (16) for decrypting said encrypted region key (RK)
- 15 using said device key (DK) in case said carrier region code (RCC) matches said device region code (RCD),
- a content reading means (17) for reading said encrypted content from said record carrier (2),
- a content decryption means (18) for decrypting said encrypted content using said decrypted region key and
- 20 - output means (19) for outputting said decrypted content.

- 2. Reproducing apparatus as claimed in claim 1,
wherein said record carrier (2) stores at least two encrypted region keys (RK),
25 wherein said device key storage means (11) is adapted for storing at least two device keys (DK),
 wherein said reproducing apparatus (1) further comprises a key selection means (15) for selecting an encrypted region key (RK) from said at least two encrypted

region keys and for selecting a device key (DK) from said at least two device keys using said carrier region code (RCC) and said device region code (RCD), and

wherein said region key decryption means (16) is adapted for decrypting said selected encrypted region key using said selected device key (DK).

5

3. Reproducing apparatus as claimed in claim 1, wherein said carrier region code (RCC) comprises one or more tags (T), each tag (T) including a revocation information (P) indicating regions from which record carriers are allowed for reproduction.

10 4. Reproducing apparatus as claimed in claim 3, wherein said tags (T) are assigned to different nodes (N) of a tree structure representing all possible regions which are at least partly combined into region groups at a node.

15 5. Reproducing apparatus as claimed in claim 4, wherein said tree structure comprises at least two hierarchical layers (L0, L1) and wherein each node (N) has a number of branches, in particular three branches.

20 6. Reproducing apparatus as claimed in claim 5, wherein a number of device keys (DK) are assigned to each node (N), said number comprising at least one device key (DK) for each branch of said node (N) which is not assigned to all other branches of said node (N).

25 7. Reproducing apparatus as claimed in claim 6, wherein said device key storage means (11) are adapted for storing only device keys (DK) assigned to nodes (N) in the chain of the hierarchical tree from the top layer (L0) to the bottom layer (L2).

30 8. Reproducing apparatus as claimed in claim 5, wherein each tag (T) includes a termination information (F) indicating if there are further tags assigned to nodes of branches, branching off from the node to which said tag (T) is assigned, in lower hierarchical layers.

9. Reproducing apparatus as claimed in claim 1, wherein said region code storage means (10), said device key storage means (11), said region code check unit (13) and said region key decryption means (16) are embedded in separate semiconductor device (100).

10. Reproducing apparatus as claimed in claim 9, further comprising a counter (30) for counting the number of times the device region code (RCD) is changed and a reset means (31) for resetting the device region code (RCD) to a default value if a predetermined number of changes has been made.

5

11. Reproducing method for reproducing content stored in encrypted form on a record carrier (2), said record carrier (2) further storing a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and an encrypted region key (RK) for decrypting said content, comprising the steps of:

- 10 - reading said carrier region code (RCC) from said record carrier (2),
- checking if said carrier region code (RCC) matches a device region code (RCD) stored in a reproduction apparatus (1),
- reading said encrypted region key (RK) from said record carrier (2),
- decrypting said encrypted region key (RK) using a device key (DK) stored in said
15 reproduction apparatus (1) in case said carrier region code (RCC) matches said device region code (RCD),
- reading said encrypted content from said record carrier (2),
- decrypting said encrypted content using said decrypted region key (RCD) and
- outputting said decrypted content.

20

12. Record carrier (2) storing

- content in encrypted form for reproduction by reproducing apparatus (1),
- a carrier region code (RCC) indicating in which region said content shall be allowed to be reproduced and
25 - an encrypted region key (RK) for decrypting said content,
wherein during reproduction
said carrier region code (RCC) is used to check if said carrier region code (RCC) matches a device region code (RCD) stored in a reproduction apparatus (1),
said encrypted region key (RK) is decrypted using a device key (DK) stored in
30 said reproduction apparatus (1) in case said carrier region code (RCC) matches said device region code (RCD), and
said encrypted content is decrypted using said decrypted region key.

13. Computer program comprising program code means for causing a computer to perform the steps of the method as claimed in claim 11 when said computer program is executed on a computer.